Course Syllabus

Title: Basic Penetration Testing and Ethical Hacking
Duration: 12 Weeks
Instructor: Songpon TEERAKANOK, *D. Eng.*
CompTIA CSIE & CTT+, ISC2 CC, Cisco CBROPS, SBT BTL1

Course Description:

This course provides a foundational understanding of ethical hacking and penetration testing. Students will learn to identify, exploit, and mitigate vulnerabilities using industry-standard and open-source tools and techniques. Topics include Unix and Kali Linux basics, reconnaissance, network scanning, password attacks, exploitation, post-exploitation strategies, and web application security. Practical assessments, including a midterm exam and final presentations, will ensure hands-on experience in ethical hacking principles and advanced exploitation methods.

Prerequisites:

Students are expected to have:
- Basic computer networks and OS knowledge
- Command-line experience
- Core cybersecurity concepts (CIA Triad)
- Commitment to hands-on learning

Tentative Course Ouline:

Week	Topic
1	Introduction to Ethical Hacking and Penetration Testing
2	Unix and Kali Linux
3	Information Gathering and Reconnaissance Techniques
4	Network Scanning, Enumeration and Vulnerability Assessment
5	Password Attacks
6	Exploitation Basics
7	Post-Exploitation Techniques
8	Midterm Exam
9	Web Application Testing I
10	Web Application Testing II
11	Advanced Exploitation Techniques
12	Final Presentations and Wrap-Up

Note *** *Topics are subject to change without prior notice.*

*** Ethical and Legal Compliance ***:

Students must follow ethical guidelines and use skills only within legal boundaries. All course activities are for educational purposes only, and any misuse is prohibited.